

## REMARKS

Claims 1-30 are pending in the present application, of which claims 1, 26, 27 and 29 are independent. No amendments have been made. Applicant believes that the present application is in condition for allowance, which prompt and favorable action is respectfully requested.

### I. REJECTION UNDER 35 U.S.C. §102

The Examiner rejected claims 1, 2, 4, 14, 16 and 26 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,587,562 issued to Jansen et al. (hereinafter "Jansen"). The Examiner also rejected claim 27 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 5,546,464 issued to Raith et al. (hereinafter "Raith"). The rejection is respectfully traversed in its entirety.

To anticipate a claim under 35 U.S.C. §102(e), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (see MPEP §2131).

Jansen discloses a synchronous data-stream generator for an encryptor and/or decryptor station. This data-stream generator comprises a plurality of subgenerators  $M_1$  to  $M_i$ , each receiving a clock trigger. In response to the clock trigger, each subgenerator provide a data item  $DS_i$ . A combining means combines data items output from the subgenerators to generate a data stream. A control means, also in response to the clock trigger, causes a selected one of the subgenerators to provide at the output the  $n_i$ th data item successive to a last data item. (See Jansen, col. 4, lines 7-20 and lines 42-58). The clock trigger and the control means are used to introduce non-linearity in the system. (Col. 1, line 66 to col. 2, line 1).

Jansen also discloses that the subgenerators may be implemented by feedback shift registers. (See Jansen, col. 5, lines 53-67). However, Jansen does not disclose using a control set of numbers to determine the current state of the stream cipher.

Moreover, assuming the clock trigger input can be equated with the control set of numbers, although the Applicant submits that they cannot be equated, the clock trigger inputs of Jansen are used only internally at either an encryptor or decryptor station. Therefore, Jansen does not disclose transmitting the control set of numbers from a transmission source.

Accordingly, Jansen does not disclose transmitting a control set of numbers and using the control set of numbers to determine the current state of the stream cipher as in independent claim 1. Furthermore, with respect to claim 2 and independent claim 26, Jansen does not disclose transmitting a cycle number and using the cycle number to determine the current state of a stream cipher.

With respect to independent claim 27, Raith discloses a handover message including an indication of whether or not cipher resynchronization is required. In Raith, synchronization is achieved by continuously transmitting from the encoding system to the decoding system, the contents of the memory device, such as bit, block or message counters, which participates in the generation of the keystream bit. (See Raith, col. 12, lines 10-23). In other words, a count of the number of keystream bits or blocks of keystream bits generated is maintained or stored. Synchronization is then achieved by transmitting this count value. Moreover, Raith does not disclose or even suggest the use of a common recurrence relation.

Accordingly, Raith does not disclose the offset as in independent claim 27. Therefore, Raith does not disclose determining the offset, transmitting the offset, and/or using the offset to calculate a new current state of a stream cipher as in independent claim 27.

Since the respective reference does not teach every element of independent claims 1, 26 and 27 in as complete detail as is contained in the claims, Applicant respectfully requests a withdrawal of the rejection under 35 U.S.C. §102 for at least the foregoing

reasons. Also, Applicant submits that claims 2, 4, 14 and 16 are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein.

## **II. REJECTION UNDER 35 U.S.C. §103**

The Examiner rejected claims 3 and 15 under 35 U.S.C. §103 as being unpatentable over Jansen in view of Raith. The Examiner also rejected claims 8-10, 20 and 21 under 35 U.S.C. §103 as being unpatentable over Jansen in view of U.S. Patent No. 4,803,339 issued to Bright et al. (hereinafter "Bright") Furthermore, claim 29 was rejected under 35 U.S.C. §103 as being unpatentable over Raith in view of Jansen.

To establish a prima facie case of obviousness for a claimed invention, all the claim elements must be taught or suggested by the prior art. (MPEP 2143.03)

With respect to claims 3, 8-10, 15, 20 and 21, Applicant submits that neither Jansen, Raith nor Bright, separately or combined, discloses all the claim elements of the independent claim 1. Therefore, Applicant submits that the claims are allowable based on their dependency from an allowable base claim as well as other novel features included therein.

With respect to claim 29, Applicant submits that neither Raith nor Jansen, separately or combined, discloses the offset as discussed above. Therefore, neither Raith nor Jansen, separately or combined, discloses determining an offset, transmitting the offset and using the offset to calculate a new current state of a stream cipher as claimed.

Since the prior art does not teach or suggest all the claim elements, Applicant respectfully requests a withdrawal of the rejection under 35 U.S.C. §103 for at least the foregoing reasons.

**III. ALLOWABLE SUBJECT MATTER**

Applicant thanks the Examiner for indicating that claims 5-7, 11-13, 17-19, 23-35, 28 and 30 contain allowable subject matter. However, Applicant would prefer to defer rewriting the claims to include the elements of the parent claim and all intervening claims until the time at which final disposition of all claims is required.

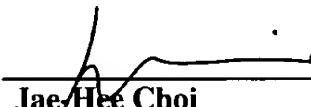
**CONCLUSION**

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: January 13, 2004

By:   
**Jae Hee Choi**  
Attorney for Applicants  
Registration No. 45,288

QUALCOMM Incorporated  
Attn: Patent Department  
5775 Morehouse Drive  
San Diego, California 92121-1714  
Telephone: (858) 651-1179  
Facsimile: (858) 658-2502